

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-315177

(43)Date of publication of application : 14.11.2000

(51)Int.Cl.

G06F 12/14

G06F 17/30

H04N 5/91

(21)Application number : 11-124182

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 30.04.1999

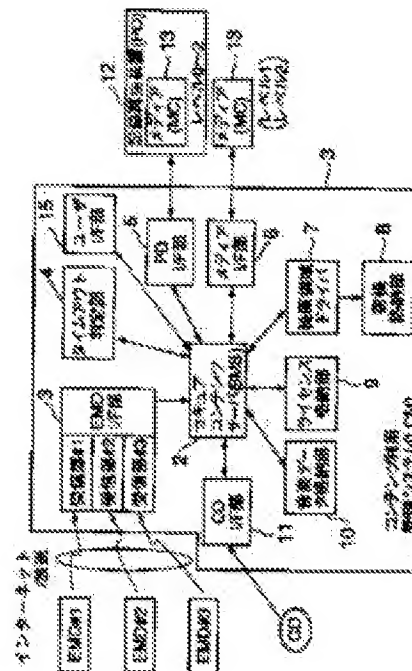
(72)Inventor : TAMURA MASABUMI  
KAMIBAYASHI TATSU  
YAMADA HISASHI  
ISHIBASHI YASUHIRO  
KATO HIROSHI  
TOMA HIDEYUKI

## (54) METHOD AND DEVICE FOR CONTENTS MANAGEMENT

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To obtain the contents managing method which limits the duplication of contents and protects the copyright of the contents by checking out from the number of contents which can be copied each time duplicate contents are recorded on a storage medium when an indication for duplicate recording to the storage medium is received.

**SOLUTION:** An LCM 1 is equipped with a secure contents server(SMS) 2 and contents are stored on an SMS 2. The SMS 2 outputs contents data to media (MC) 13. The SMS 2 subtracts '1' from the rest number of contents of checkout requests of a hotel book and erases information stored in areas corresponding to the folders of the contents on the MC 13 by overwriting random numbers. Then the SMS 2 receives the values of the respective areas after overwriting transferred from the MC 13 so as to confirm the overwriting erasure and checks them. Consequently, the number of duplicate contents is efficiently restricted to protect the copyright of the contents.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2000-315177  
(P2000-315177A)

(43)公開日 平成12年11月14日 (2000. 11. 14)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
			3 2 0 B 5 B 0 7 5
17/30		15/40	3 2 0 Z 5 C 0 5 3
H 0 4 N 5/91			3 7 0 G
		H 0 4 N 5/91	P
審査請求 未請求 請求項の数14 O L (全 20 頁)			

(21)出願番号 特願平11-124182

(22)出願日 平成11年4月30日 (1999. 4. 30)

(71)出願人 000003078

株式会社東芝  
神奈川県川崎市幸区堀川町72番地

(72)発明者 田村 正文

東京都港区芝浦一丁目1番1号 株式会社  
東芝本社事務所内

(72)発明者 上林 達

神奈川県川崎市幸区小向東芝町1番地 株  
式会社東芝研究開発センター内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

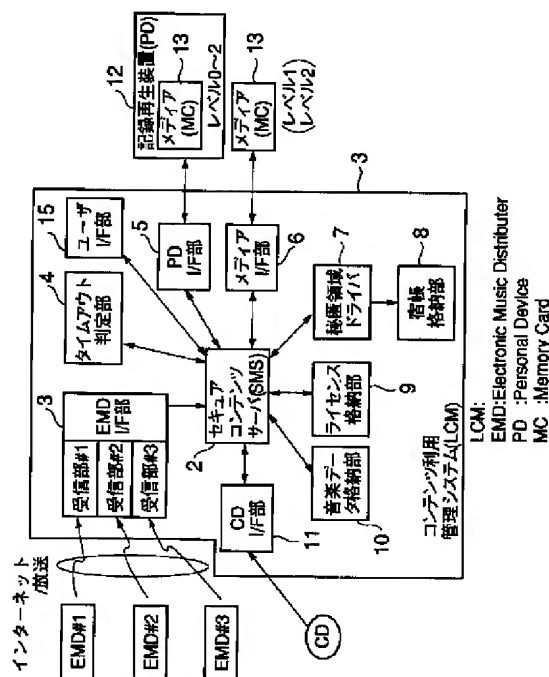
最終頁に続く

(54)【発明の名称】 コンテンツ管理方法およびコンテンツ管理装置

(57)【要約】

【課題】記憶媒体に記録できる複製コンテンツの数を規制することによりコンテンツの複製を制限して、コンテンツの著作権を保護することのできるコンテンツ管理方法を提供する。

【解決手段】記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを1つ記録する毎に前記複製可能コンテンツ数から1減算し、また、該記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを1つ消去する毎に前記複製可能コンテンツ数を1加算することを特徴とするコンテンツ管理方法。



## 【特許請求の範囲】

【請求項1】 記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを1つ記録する毎に前記複製可能コンテンツ数から1減算し、また、該記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを1つ消去する毎に前記複製可能コンテンツ数を1加算することを特徴とするコンテンツ管理方法。

【請求項2】 前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報を記録することを特徴とする請求項1記載のコンテンツ管理方法。

【請求項3】 前記コンテンツ毎の少なくとも前記複製可能コンテンツ数を秘匿された特定手続にてアクセス可能な秘匿記憶領域に記録することを特徴とする請求項1記載のコンテンツ管理方法。

【請求項4】 前記コンテンツ毎の少なくとも前記複製可能コンテンツ数と複製コンテンツを記憶した記憶媒体の識別情報とを秘匿された特定手続にてアクセス可能な秘匿記憶領域に記憶し、前記秘匿記憶領域に前記記憶媒体の識別情報が記憶されているときのみ該記憶媒体から該複製コンテンツを消去することを特徴とする請求項1記載のコンテンツ管理方法。

【請求項5】 前記記憶媒体に前記複製コンテンツを記録する際、該記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報と該複製コンテンツの移動の可否を表すフラグ情報とを記録し、該フラグ情報を参照して、該複製コンテンツの移動の可否を判断することを特徴とする請求項1記載のコンテンツ管理方法。

【請求項6】 前記記憶媒体に対するデータの読み出しあるいは書き込み処理にかかる時間が所定時間以内でないとき、以降の処理を中断することを特徴とする請求項1記載のコンテンツ管理方法。

【請求項7】 前記記憶媒体として、その記憶領域内に、秘匿された特定の手続のみにてアクセス可能な秘匿領域が設けられるとともに該記憶媒体の識別情報が記憶された第1の種別の記憶媒体と、前記秘匿領域を具備しないが該記憶媒体の識別情報は有している第2の種別の記憶媒体と、前記秘匿領域および該記憶媒体の識別情報を持たない第3の種別の記憶媒体とがあり、前記記憶媒体に複製コンテンツを記録する際および該記憶媒体から複製コンテンツを消去する際および該記録媒体に記憶された複製コンテンツを再生する際には、該記憶媒体の種

別を判別してから、それに応じた処理を施すことを特徴とする請求項1記載のコンテンツ管理方法。

【請求項8】 記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理装置であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを1つ記録する毎に前記複製可能コンテンツ数から1減算する複製コンテンツ記録手段と、前記記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを1つ消去する毎に前記複製可能コンテンツ数を1加算する複製コンテンツ移動手段と、を具備したことを特徴とするコンテンツ管理装置。

【請求項9】 前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報を記録することを特徴とする請求項8記載のコンテンツ管理装置。

【請求項10】 前記コンテンツ毎の少なくとも前記複製可能コンテンツ数を秘匿された特定手続にてアクセス可能な秘匿記憶領域に記録することを特徴とする請求項8記載のコンテンツ管理装置。

【請求項11】 前記コンテンツ毎の少なくとも前記複製可能コンテンツ数と複製コンテンツを記憶した記憶媒体の識別情報とを秘匿された特定手続にてアクセス可能な秘匿記憶領域に記憶し、前記秘匿記憶領域に前記記憶媒体の識別情報が記憶されているときのみ該記憶媒体から該複製コンテンツを消去することを特徴とする請求項8記載のコンテンツ管理装置。

【請求項12】 前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報と該複製コンテンツの移動の可否を表すフラグ情報とを記録し、該フラグ情報を参照して、該複製コンテンツの移動の可否を判断することを特徴とする請求項8記載のコンテンツ管理装置。

【請求項13】 前記記憶媒体に対するデータの読み出しあるいは書き込み処理にかかる時間が所定時間以内でないとき、以降の処理を中断することを特徴とする請求項8記載のコンテンツ管理装置。

【請求項14】 前記記憶媒体に複製コンテンツを記録する際および該記憶媒体から複製コンテンツを消去する際および該記録媒体に記憶された複製コンテンツを再生する際には、前記記憶媒体が、その記憶領域内に秘匿された特定手続にてアクセス可能な秘匿領域が設けられるとともに該記憶媒体の識別情報が記憶された第1の種別の記憶媒体か、前記秘匿領域を具備しないが該記憶媒体の識別情報は有している第2の種別の記憶媒体か、前記秘匿領域および該記憶媒体の識別情報を持たない第3の

種別の記憶媒体のうちのいずれであるかを判別する判別手段を具備し、この判別手段で判別された前記記録媒体の種別に応じた処理を施すことを特徴とする請求項8記載のコンテンツ管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、記憶媒体に記憶できる音楽や映画等の複製コンテンツの数を規制するためのコンテンツ管理方法およびそれを用いたコンテンツ管理装置に関する。

【0002】

【従来の技術】従来、コンテンツ（著作物等）は、コピー管理が行われてきた。コピー世代管理やコピーの数を管理する事により、著作権保護と利用の便宜のバランスをとってきた。

【0003】さらに、コピー管理に代わって、「移動」の概念が登場してきた。コピーがオリジナルのデータを消去しないのと同様に、移動は、異なった場所（メディア）にデータを転送すると共に、オリジナルデータを消去する。コンテンツのデジタル化とネットワーク等の普及が、移動によるコピープロテクションが登場した背景にある。

【0004】

【発明が解決しようとする課題】近年、ネットワーク等を通じたオリジナルの忠実なコピーが可能になったため、コピー管理だけでは、著作権保護が困難になってきた。また、メディアからメディアへの無制限な移動、例えば、データの営利目的（移動による）配布は、著作権管理を行うことができない。

【0005】このように、オリジナルのデータ（特に、著作権保護の対象となるようなコンテンツ）の複製を確実に管理することが困難となってきた。

【0006】そこで、本発明は、上記問題点を鑑み、記憶媒体に記録できる複製コンテンツの数を規制することによりコンテンツの複製を制限して、コンテンツの著作権を保護することのできるコンテンツ管理方法およびそれを用いたコンテンツ管理装置を提供することを目的とする。

【0007】

【課題を解決するための手段】1.（請求項1：チェックイン／チェックアウト）本発明のコンテンツ管理方法は、記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを1つ記録する毎に前記複製可能コンテンツ数から1減算し（チェックアウト）、また、該記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該

複製コンテンツを1つ消去する毎に前記複製可能コンテンツ数を1加算する（チェックイン）ことを特徴とする。

【0008】（請求項8）本発明のコンテンツ管理装置は、記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理装置であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを1つ記録する毎に前記複製可能コンテンツ数から1減算する複製コンテンツ記録手段と、前記記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを1つ消去する毎に前記複製可能コンテンツ数を1加算する複製コンテンツ移動手段とを具備したことを特徴とする。

【0009】本発明によれば、複製コンテンツの数を効率よく規制することができる。

【0010】2.（請求項2、9：記憶媒体に秘匿領域を設ける）好ましくは、前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報（例えば、暗号化されたコンテンツ復号鍵を復号するために必要な乱数r）を記録することを特徴とする。

【0011】これにより、記憶媒体内の秘匿領域に記録されたデータ（例えば乱数r）は、特定手続（例えば、認証による正当性の確認）が行えない別の記憶媒体に退避する事はできない。従って、例えば「TID1」というコンテンツのチェックイン後、記憶媒体に復帰されたコンテンツを利用する事はできなくなるので複製コンテンツ管理のための信頼性が向上する。

【0012】3.（請求項3、10：宿帳を秘匿領域に記憶する）好ましくは、前記コンテンツ毎の少なくとも前記複製可能コンテンツ数を秘匿された特定手続にてアクセス可能な秘匿記憶領域に記録することを特徴とする。

【0013】これにより、秘匿領域に記憶される宿帳（コンテンツ毎の少なくとも複製可能コンテンツ数（子の残数）を登録したもの）は、特定手続（例えば、認証による正当性の確認）が行えない別の記憶媒体に退避する事はできない。従って、例えば「TID1」というコンテンツをチェックアウトした後で、宿帳をチェックアウト前の状態に戻す事はできなくなるので、複製コンテンツ管理のための信頼性が向上する。

【0014】4.（請求項4、11：宿帳のチェックアウトリストにのっている記憶媒体のみがチェックイン可）好ましくは、前記コンテンツ毎の少なくとも前記複製可能コンテンツ数と複製コンテンツを記憶した記憶媒体の識別情報とを（宿帳として）秘匿された特定手続にてアクセス可能な秘匿記憶領域に記憶し、前記秘匿記憶

領域に前記記憶媒体の識別情報が記憶されているときのみ該記憶媒体から該複製コンテンツを消去することにより、より厳密に複製コンテンツの管理が行える。

【0015】5. (請求項5、12: フラグによるチェックインの制限) 好ましくは、前記記憶媒体に前記複製コンテンツを記録する際、該記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報と該複製コンテンツの移動の可否を表すフラグ情報とを記録し、該フラグ情報を参照して、該複製コンテンツの移動の可否を判断する。

【0016】例えば宿帳にない記憶媒体からの複製コンテンツのチェックインを可能にすると、コンテンツの中古市場が成立する原因を作ることにもなる。この対策として、記憶媒体の秘匿領域にチェックインを制限するためのフラグ情報を記録し、複製コンテンツのチェックインを行う際に、まず、当該記憶媒体から読み出したフラグ情報をチェックしてチェックインが可能であるか否かを確認する。そして、可能であると判断されたときのみ、チェックインを行うことにより、コンテンツ毎にチェックインを容易にコントロールできる。

【0017】6. (請求項6、13: ネットワークを介する記憶媒体への複製コンテンツの記録を制限) 好ましくは、前記記憶媒体に対するデータの読み出しあるいは書き込み処理にかかる時間が所定時間以内でないとき、以降の処理を中断することにより、ネットワークを介した違法な複製コンテンツの配信を未然に防ぐことができ、複製コンテンツの作成をより厳密に規制することができる。

【0018】7. (請求項7、14: 記憶媒体の種別を判別してからチェックイン、チェックアウト、再生処理を行う) 好ましくは、前記記憶媒体として、その記憶領域内に、秘匿された特定の手続のみにてアクセス可能な秘匿領域が設けられるとともに該記憶媒体の識別情報が記憶された第1の種別(レベル2)の記憶媒体と、前記秘匿領域を具備しないが該記憶媒体の識別情報は有している第2の種別(レベル1)の記憶媒体と、前記秘匿領域および該記憶媒体の識別情報を持たない第3の種別(レベル0)の記憶媒体とがあり、前記記憶媒体に複製コンテンツを記録する際および該記憶媒体から複製コンテンツを消去する際および該記憶媒体に記憶された複製コンテンツを再生する際には、該記憶媒体の種別を判別してから、それに応じた処理を施すことを特徴とする。

【0019】これにより、従来からある構成の記憶媒体(レベル0やレベル1)を用いてチェックイン/チェックアウトによる複製コンテンツの管理も容易に行える。

【0020】

【発明の実施の形態】以下、本発明の実施形態について、図面を参照して説明する。図1は、本実施形態にかかる記憶媒体(メディア)に記憶できる複製コンテンツ

の数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム(以下、簡単にLCMと呼ぶことがある)1の構成例を示したものである。なお、ここでは、コンテンツとして音楽を一例として用いているが、この場合に限らず、映画や、ゲームソフト等であってもよい。また、メディアとしてメモ리카ード(MC)を用いているが、この場合に限るものではなく、フロッピー(登録商標)ディスク、DVD等の各種記憶媒体であってもよい。

【0021】EMD(Electronic Music Distributor)は、音楽配信サーバまたは音楽配信放送局である。コンテンツ利用管理システム1は、例えば、パソコン(PC)であり、複数のEMD(ここでは、EMD#1~#3)に対応した受信部#1~#3を具備しており、EMDが配信する暗号化コンテンツまたはそのライセンス(利用条件と暗号化コンテンツ復号鍵)などを受信する。受信部#1~#3は、再生機能や課金機能を有して居ても良い。配信された音楽コンテンツを試聴する為に再生機能が利用される。又、課金機能を利用して、気に入ったコンテンツを購入する事が可能である。

【0022】LCM1は、セキュア・コンテンツ・サーバ(ここでは、Secure Music Server: SMSで、以下、簡単にSMSと呼ぶことがある)2を具備し、利用者が購入したコンテンツはEMDインタフェース(I/F)部3を経由してSMS2に蓄積される。音楽コンテンツは、必要に応じてEMDI/F部3で復号され、形式変換や再暗号化が施される。SMS2が暗号化コンテンツを受け取ると、それを音楽データ格納部10に格納し、音楽データ復号鍵をライセンス格納部9に格納する。SMS2が再生機能を有して居ても良い。当該再生機能により、SMS2が管理する音楽コンテンツをPC上で再生する事ができる。

【0023】SMS2は、メディア(以下、簡単にMC(memory card)と呼ぶことがある)13に対してコンテンツデータを出力する機能を有している。MC13を記録再生装置(以下、簡単にPD(Portable Device)と呼ぶことがある)12にセットし、MC13に記録されたコンテンツを再生することができる。

【0024】SMS2からMC13へのコンテンツの記録はメディア(MC)インタフェース(I/F)部6を通じて直接行われるか、又はPD12を経由して行うことができる。

【0025】MC13は、そのメディア固有かつ書き換え不能の識別情報(MID)を有しており、MC13に格納されるコンテンツは、MC13に依存するコンテンツ復号鍵で暗号化される。

【0026】コンテンツ復号鍵は、メディアI/F部6およびPD12内部に格納されている暗号鍵Kpによって暗号化され、MC13に記録される。

【0027】MC13内のコンテンツ及びコンテンツ復

号鍵は、別個の任意の記憶媒体（以下、MCbと呼ぶ）にコピーする事が可能であるが、

1. 正統なPD12のみが暗号鍵Kpを有する事から、MCbに格納されたコンテンツは正統なPD12でなければ正しく再生されない。ところが、
2. MC13の識別情報MIDはコピーできない事から、MCbの識別情報MIDはコピー元のMC13の識別情報MIDとは異なっており、結局、MCbにコピーされたコンテンツを正しく再生する事はできない。すなわち、SMS2がMC13に記録した複製コンテンツが、次々と別のMCにコピーされ利用される事が防止されている。

【0028】以上が従来から考えられているLCM1の構成であるが、次に、本発明にかかる方法および構成部について説明する。

【0029】まず、チェックイン／チェックアウトについて、図1のLCM1に則して説明する。

【0030】チェックアウトとは、LMS1が「親」としてのコンテンツを格納しており、MC13に、その複製を「子」コンテンツとしてコピーすることをいう。

「子」コンテンツはPD12で自由に再生する事が可能であるが、「子」から「孫」コンテンツを作成する事は許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、MC13をLCM1に接続し、LCM1が「子」コンテンツを消去（又は利用不能）する事で、LCM1内の「親」コンテンツは「子」を1つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【0031】このチェックイン／チェックアウトを単純に、従来からのLCM1で実現しようとする、と、実際、次の様な「攻撃」が存在する。すなわち、MC13に格納された「子」を別の記憶メディアに（MIDを除いて）退避しておき、MC13の「子」を「親」にチェックインする。次いで、先に退避しておいた「子」を当該MC13に書き戻す。既にチェックインは済んでいるので、LCM1上の「親」は別のMC13に「子」をコピーして良い。この方法で、任意の個数だけ利用可能な「子」を作る事が可能である。

【0032】上述の「攻撃」には、MC13とLCM1とのデータ転送の際に認証を行う事により、対抗可能である。すなわち、MC13は正当なLCM1以外からのデータ転送を受け付けず、LCM1が正当なMC13以外からのデータ転送を受け付けずと仮定する。この場合、MC13内の「子」を別の記録メディアに退避する事はできない。又、LCM1に対して、偽って、チェックインすることもできない。従って、上述の「攻撃」は破綻する。

【0033】ところが、実は、LCM1とMC13との認証を前提としても、チェックイン／チェックアウトは

実現できない。次の様な「攻撃」が存在するからである。すなわち、まず、LCM1上の「親」が「子」を作っていない状態で、LCM1のデータ（特に、ライセンス格納部9の情報）を別の記憶メディアにバックアップする。MC13に「子」をコピーした後、バックアップしたLCM1のデータを復帰する。LCM1の「親」は「子」を作る前の状態に戻るから、別のMC13に「子」を作成する事ができる。この様にして、任意の数の「子」を作成する事が可能となってしまう。

【0034】次に、チェックイン／チェックアウトを実現する上で生じる問題点以外の問題点について説明する。すなわち、インターネット等の所定の通信路を経由したMC13への記録である。EMDによる正規のインターネット配信は、著作権所有者の許諾を得て行う正当な配信であるから問題は無い。ところが、図21の様な形態で、インターネット経由でMC13へのコンテンツの記録を行う事ができてしまう。図21におけるパソコン（PC）上の通信部201は、単にMC13への書き込みプロトコルを中継しているだけである。LCM1は、当該LCM1が稼働するPC#2に直接接続されているPD12と、通信部201を介してリモート接続されているLCM1の稼働するPC#2に接続されているPD12とを区別する事ができない為、インターネット等のネットワークを介したコンテンツの（違法な）配布が可能である。

【0035】以下、本発明の要旨である、チェックイン／チェックアウトと、ネットワークを介するMC13へのコンテンツ記録を規制するための手段等について、次に示す項目の順に説明する。

【0036】1. チェックイン／チェックアウト

(1-1) チェックイン／チェックアウト

(1-2) レベル2のMCを用いた複製コンテンツのチェックイン／チェックアウト

(1-3) 宿帳による複製コンテンツの他の管理方法

(1-4) レベル2のMCに記憶された複製コンテンツの再生

(1-5) レベル1のMCを用いた複製コンテンツのチェックイン／チェックアウト、複製コンテンツの再生

(1-6) レベル0のMCを用いた複製コンテンツのチェックイン／チェックアウト、複製コンテンツの再生

2. ネットワークを介するMCへの複製コンテンツの記録を規制するための手段

3. 秘匿領域

(チェックイン／チェックアウト) チェックイン／チェックアウトを実現するために、MC13内の記憶領域に、公開された手順では読み書きできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録する（図2参照）。また、LCM1の記憶領域（例えば、LCM1がPCで構成されている場合には、ハードディスク（HDD））上に非公開の手順でしかアクセス

できない領域（秘匿領域）を設け、後述するような宿帳を当該秘匿領域に格納する（図2参照）。さらに、PD 12の記憶領域上にも非公開の手順でしかアクセスできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録するようにしてもよい（図2参照）。なお、ここでは、記憶領域中の秘匿領域以外の通常に手順にてアクセス可能な領域を公開領域と呼ぶ。

【0037】図1に示すように、LCM1では、秘匿領域には、宿帳格納部8が設けられ、SMS2にてこの宿帳格納部8にアクセスするための秘匿された特定の手段が行われた後、秘匿領域からデータを読み取るための秘匿領域ドライバ7を具備している。

【0038】図4（c）に示すように、MC13は、その識別情報MIDを格納するための外部からは書換不可能で、コピーも不可能なような構成になっている識別情報格納部13bと、秘匿領域13cと、公開領域13aと、秘匿領域13cにアクセスされる度に認証部13dにて認証を行って、正当な相手であると確認されたときに初めて秘匿領域13cにアクセス可能なようにゲートを開くスイッチ（SW）13eを具備する。なお、本実施形態で利用可能なMC13は、3種類あり、図4（c）に示すような、識別情報MIDと秘匿領域とを両方兼ね備えているMC13の種別を「レベル2」と呼ぶ。秘匿領域は持たないが識別情報MIDは持つ図4（b）に示すようなMC13の種別を「レベル1」と呼ぶ。秘匿領域も識別情報も持たない図4（a）に示すようなMC13の種別を「レベル0」と呼ぶことにする。これら種別は、例えば、識別情報MIDの有無でレベル0とそれ以外の種別とが判別でき、さらに、識別情報MIDの構成からレベル1とレベル2とを判別する。例えば、識別情報が連続した数値であるとき、所定値以上はレベル2であるとする。

【0039】以下、特に断らない限り、レベル2のMC13の場合を例にとり説明する。

【0040】このMC13は、LCM1に接続されたPD12にセットして用いる場合とLCM1に直接セットして用いる場合とがある。

【0041】図3は、PD12の構成例を示したもので、MC13は、メディアインタフェース（I/F部）12fにセットされる。LCM1がPD12を介してMC13に読み書きする場合は、PD12内の秘匿領域アクセス部を経由してMC13の秘匿領域にアクセスする。メディアI/F部12fには、MC13の秘匿領域にアクセスするための秘匿領域アクセス部を具備している。PD12内の秘匿領域は、フラッシュメモリ12dに設けられていても良い。ROM12cには、MC13との間で相互認証を行うためのプログラムや、MC13の種別を判別するためのプログラムも書き込まれていて、このプログラムに従って、CPU12aの制御の下、MC13との間の相互認証、種別判別等の処理を実行する

ようになっている。

【0042】図5は、LCM1のメディアI/F部6の構成を示したもので、MC13との間で相互認証を行うための認証部6cと、MC13の種別を判別するメディア判別部6bと、これら全体を制御するための制御部6aとから構成されている。認証部6cは、MC13の秘匿領域にアクセスするための秘匿領域アクセス部である。

【0043】次に、LCM1の秘匿領域に格納される宿帳について説明する。

【0044】SMS2にて保持する全ての音楽コンテンツは、そのそれぞれを識別するための識別情報であるコンテンツID（TID）と、予め定められた複製可能コンテンツ数、すなわち、子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼ぶ。宿帳は、秘匿領域に設けられた宿帳格納部8に図7（a）に示すような形態で記録されている。

【0045】図7（a）において、例えば、コンテンツID「TID1」なる子の残数は「2」で、そのチェックアウトリストはL1である。

【0046】チェックアウトリストは、複製コンテンツ（子）を記録したMC13の識別情報のリストであって、例えば、図7（a）において、チェックアウトリストL1には「m1」と「m2」という識別情報を持つ2つのMC13にコンテンツID「TID1」なるコンテンツの子がチェックアウトされていることがわかる。

【0047】（レベル2のMCを用いた複製コンテンツのチェックイン／チェックアウト）次に、図4（c）に示したような構成のレベル2のMC13を用いたチェックイン／チェックアウトについて、図9～図11を参照して説明する。

【0048】MC13がLCM1のメディアI/F部6、あるいは、PD12にセットされると、メディアI/F部6とMC13との間、あるいは、PD12とMC13との間で相互認証が行われ（図9のステップS1）、双方にて正当な相手であると判断されたとき（ステップS2）、メディアI/F部6あるいはPD12はMC13から読み取った識別情報MIDを基に、MC13の種別を判別する（ステップS3）。ここでは、MC13の種別は、レベル2であるので、メディアI/F部6あるいはPD12は、その種別に応じたチェックイン／チェックアウト処理を実行する（ステップS6）。

【0049】チェックアウトの指示がLCM1のユーザインタフェース（I/F）部15を介して、あるいは、PD12を介して、SMS2になされた場合について、図10を参照して説明する。SMS2は、宿帳のチェックアウト要求のあったコンテンツ（例えばコンテンツIDが「TID1」であるとする）の子の残数nを調べ（ステップS101）、n>0のとき、必要があれば、MC13との間で相互認証を行い（ステップS10



2)、相互に正当性が確認されたら、次に、MC13から、その識別情報MID(例えば、MID=m0とする)を転送してもらう(ステップS103)。

【0050】SMS2では、乱数rを発生し、この乱数rと、MC13の識別情報m0と、正当なるMC13とLCM1との間で共有する鍵生成アルゴリズムWと用いて、暗号化鍵wを生成する。なお、鍵生成アルゴリズムWは、2つの引数(ここでは、rとm0)をとり、暗号化鍵wを毎回変化させる役割を果たす。さらに、SMS2では、暗号化されたコンテンツを復号するためのコンテンツ復号鍵K(C)をMC13とLCM1との間で共有する暗号鍵Kpと先に生成した暗号化鍵wとで暗号化する。それをw[Kp[k(C)]]と表す。また、コンテンツCを鍵K(C)で暗号化する。それをK(C)[C]と表す(ステップS104)。

【0051】SMS2は、MC13の記憶領域に、例えば「TID1」という名前のフォルダを作成すると(ステップS105)、当該フォルダの公開領域に暗号化されたコンテンツK(C)[C]と、暗号化されたコンテンツ復号鍵w[Kp[k(C)]]とを書き込む(ステップS106、ステップS107)。

【0052】次に、SMS2は、MC13の秘匿領域13cにアクセスすべく、MC13との間で相互認証を行い、双方の正当性が確認されてスイッチ13eにより秘匿領域13cへのゲートが開かれると、乱数rを秘匿領域13c内のフォルダ「TID1」に対応する領域に書き込む(ステップS108～ステップS109)。それが終了すると秘匿領域13cへのアクセスを可能にしていたゲートがスイッチ13eにより閉じられる仕組みになっている。また、ステップS108において、乱数rを秘匿領域13cに転送するまでの経路は、乱数rを暗号化する等して転送保護することが望ましい。

【0053】最後に、SMS2は、図7(b)に示すように、宿帳のチェックアウト要求のあったコンテンツID「TID1」のコンテンツの子の残数nから「1」減算し、チェックアウトリストL1に、当該MC13の識別情報「m0」を追加する(ステップS110)。

【0054】以上の処理が終了したときのMC13の記憶内容を図6に示す。

【0055】チェックインの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介して、SMS2になされた場合について、図11を参照して説明する。

【0056】SMS2は、必要があれば、MC13との間で相互認証を行い(ステップS201)、相互に正当性が確認されたら、次に、MC13から、その識別情報MID(例えば、MID=m0とする)を転送してもらう(ステップS202)。

【0057】SMS2は、チェックイン要求のなされたコンテンツ(例えばコンテンツIDが「TID1」であ

るとする)の宿帳から、そのチェックアウトリストに当該MC13の識別情報、すなわち、ここでは、「m0」が登録されているとき、乱数r1、r2を発生させる(ステップS203)。そして、MC13の公開領域13aの当該コンテンツのフォルダ(ここでは、フォルダ「TID1」)に対応する領域に記憶されている情報を乱数r2で上書きすることで消去し(ステップS204)、また、SMS2は、MC13の秘匿領域13cにアクセスすべく、MC13との間で相互認証を行い、双方の正当性が確認されてスイッチ13eにより秘匿領域13cへのゲートが開かれると、秘匿領域13c内のフォルダ「TID1」に対応する領域を乱数r1で上書きすることで消去する(ステップS205)。それが終了すると秘匿領域13cへのアクセスを可能にしていたゲートがスイッチ13eにより閉じられる仕組みになっている。また、ステップS205において、乱数r1を秘匿領域13cに転送するまでの経路は、乱数r1を暗号化する等して転送保護することが望ましい。

【0058】その後、SMS2では、上書き消去の確認をすべく、MC13から上書き後の各領域の値を転送してもらい(ステップS206)、それが数r1、r2と一致するかどうかチェックする(ステップS207)。上書き消去の確認がなされたら、MC13からフォルダ「TID1」を消去する(ステップS208)。

【0059】最後に、図7(c)に示すように、宿帳のチェックイン要求のあったコンテンツID「TID1」のコンテンツの子の残数nに「1」加算し、チェックアウトリストL1から、当該MC13の識別情報m0を削除する(ステップS209)。

【0060】MC13内の秘匿領域13cに記録された乱数rは、(認証による正当性が確認できないので)別の記憶メディアに退避する事はできない。従って、「TID1」というコンテンツのチェックイン後、MC13に復帰されたコンテンツを利用する事はできない。又、LCM1の秘匿領域にて記憶される宿帳も(認証による正当性が確認できないので)別の記録メディアに退避する事ができない。従って、「TID1」というコンテンツをチェックアウトした後で、宿帳をチェックアウト前の状態に戻す事はできない。この様に、本発明は先述の攻撃に対する対策を提供する。

【0061】なお、チェックインの際、MC13の秘匿領域の内容を乱数で上書きする事は、セキュリティ上重要である。MC13の秘匿領域に書き込みを行い得るのは、正統なSMS2のみであるが、逆に正統なSMS2は、必ず秘匿手続きによって秘匿領域に書き込みを行う。秘匿手続きによる書き込みが成功する事を以って、MC13の正統性が保証される。即ち、不正なチェックインを防止する事が可能である。安全性を高めるため、SMS2は秘匿領域を任意の乱数で上書きした後、その内容を(秘匿手続きによって)読み込み、上書きした乱



数である事を確認する様にしている。

【0062】(宿帳による複製コンテンツの他の管理方法)なお、SMS2は、宿帳に無いタイトル(コンテンツID)のコンテンツをチェックインする様にしても良い。又、チェックアウトリストに無いMC13からのチェックインを認めても良い。この場合、宿帳は、各コンテンツに対するチェックアウトリストを持たない。チェックアウトリストは、「身に覚えの無い」MC13からのチェックインを防止するために参照されるものだからである。この場合の宿帳の記憶内容を図8(a)に示す。

【0063】図8(a)に示すように、各コンテンツの宿帳には、そのコンテンツIDと子の残数のみが登録されている。

【0064】今、TID7と言うコンテンツIDを有するコンテンツを、メディア識別情報MID=m0を有するMC13からチェックインする場合を考える。すなわち、当該MC13には、現在、別のSMS2からチェックアウトされたコンテンツID「TID7」なるコンテンツが、図6に示したような形態で記憶されている。

【0065】LCM1は、図11に示した手順のうち、ステップS203のチェックアウトリストの参照を行わずにMC13内の秘匿領域、公開領域の記憶内容を消去するとともに、フォルダ「TID7」を削除する。そして、宿帳に新たなコンテンツの宿帳(TID7、1)を登録する。

【0066】LCM1が宿帳に無いコンテンツをチェックインする事で、例えば次の様な事が可能になる。自宅PCにて構成されるLCM1が格納する「親」コンテンツが「子」を2つ持つ事ができるとする。自宅PCからMC13に「子」を1つチェックアウトし、友人宅のPCにチェックインする。自分が購入した「親」が「子」を作る数を1つ減らして、友人にコンテンツをプレゼントした事になる。

【0067】このように、LCM1が宿帳にないコンテンツのチェックインを可能とすると、「子」のコンテンツがLCM1を介して「移動」する事が可能である。これはユーザにとっては便利な機能であるが、コンテンツの中古市場が成立する原因を作ることにもなる。実際、次のような中古コンテンツ売買が成立する。すなわち、ユーザがEMDから新作のコンテンツを購入し、短期間所持した後に、中古データ販売店のLCM1に当該コンテンツをチェックインする。この際、当該ユーザは代金を受け取る。中古データ販売店は、別の購入希望者に、EMDの正規価格より安い値段でデータを販売する。

【0068】この様に、コンテンツの著作権をコントロールできない「中古市場」の成立は、コピーライト・ホルダーにとって好ましくない。従って、コピーライト・ホルダーが、異なったLCM1へのチェックインをコントロールできる様、各コンテンツにチェックアウト属性

フラグfを持たせても良い。

【0069】この場合のLCM1が有する宿帳の形式を図18(a)に示す。

【0070】図18(a)に示すように、各コンテンツの宿帳には、そのコンテンツIDと子の残数とチェックアウトリストとチェックアウト属性フラグfが登録されている。

【0071】フラグfが「1」の場合、当該コンテンツは他のLCM1にチェックアウト、チェックイン可能であるが、フラグfが「0」のときは、当該コンテンツは、少なくとも他のLCM1にチェックインすることはできない。

【0072】例えば、コンテンツID「TID6」というコンテンツをチェックアウトする場合を考える。まずSMS2は宿帳を調べ、当該コンテンツのチェックアウト属性フラグが「1」であることを確認する。ここでは、この値が「0」であるとき、当該LCM1では、当該コンテンツをチェックアウトしないこととする。フラグfが「1」であるときは、図10に示した手順と同様に、コンテンツID「TID6」の宿帳の子の残数から「1」減算して「1」とする(図18(b)参照)。ちなみに、チェックアウトリストL6は空(φと表記する)であり、しかもフラグfは「1」であり、当該コンテンツは他のPC上の設けられたLCM1にチェックイン可能であるから、チェックアウトリストを持つ必要がない。また、フラグfは、MC13の秘匿領域に乱数rとともに記録されるものとする。

【0073】次に、コンテンツID「TID6」というコンテンツを、チェックアウトしたLCM1と同じLCM1、あるいは別のLCM1に、チェックインする場合について、図19に示すフローチャートを参照して説明する。

【0074】図11に示した手順にて、MC13とLCM1との間で相互認証を行い(ステップS11)、MC13の識別情報MIDを取得する(ステップS12)。

【0075】SMS2は、チェックイン要求のあったコンテンツが宿帳に登録されているいにかかわらず、MC13の秘匿領域13cに前述した秘匿手続(MC13との間で相互認証を行い、双方の正当性が確認されてスイッチ13eにより秘匿領域13cへのゲートが開かれる)を行って、秘匿領域13cからフラグfを読み取る(ステップS13)。フラグfが「1」であるときは(ステップS14)、図11のステップS204～ステップS208を行い(ステップS15～16)、フラグfが「0」のときは、処理を終了する。そして、最後に、宿帳に当該コンテンツが登録されていないときは、そのコンテンツの子の残数を「1」とした「TID6」の新たな宿帳(TID6、1、φ、1)を登録し、宿帳に当該コンテンツが登録されているときは、そのコンテンツの子の残数に「1」を加算する(ステップS1

7)。

【0076】(レベル2のMCに記憶された複製コンテンツの再生)次に、図4(c)に示したような構成のレベル2のMC13に記憶された複製コンテンツの再生について、図12を参照して説明する。MC13をPD12にセットすると、PD12は、MC13から、その識別情報MID(例えば、MID=m0とする)を転送してもらう(ステップS301)。このとき、識別情報MID=m0を基に、MC13の種別を判別が、レベル2であることが判別できる。そこで、PD12は、MC13の公開領域からw[Kp[k(C)]]を読み出すとともに(ステップS302)、MC13の秘匿領域13cにアクセスすべく、MC13との間で相互認証を行い、双方の正当性が確認されてスイッチ13eにより秘匿領域13cへのゲートが開かれると、秘匿領域13c内のフォルダ「TID1」に対応する領域から乱数rを読み出す(ステップS303)。それが終了すると秘匿領域13cへのアクセスを可能にしていたゲートがスイッチ13eにより閉じられる仕組みになっている。

【0077】PD12は、乱数rと、MC13の識別情報m0と、正当なるMC13とPD12との間で共有する鍵生成アルゴリズムWを用いて、暗号化鍵wを生成する。暗号化鍵wと、MC13とLCM1との間で共有する暗号鍵Kpと、MC13から読み出されたw[Kp[k(C)]]とからコンテンツ復号鍵K(C)を復号する(ステップS304)。

【0078】そして、PD12は、MC13の公開領域から暗号化されたコンテンツK(C)[C]を読み出し(ステップS305)、復号部12gでコンテンツCを復号し、デコーダ12hでデコードして、D/A変換部でデジタル信号からアナログ信号に変換し、音楽を再生する(ステップS306)。

【0079】(レベル1のMCを用いた複製コンテンツのチェックイン/チェックアウト、複製コンテンツの再生)次に、図4(b)に示したような構成のレベル2のMC13を用いたチェックイン/チェックアウトについて、図9、図13を参照して説明する。なお、レベル1のMC13は、秘匿領域を持たないので、チェックインを行うことができない。

【0080】MC13がLCM1のメディアI/F部6、あるいは、PD12にセットされてから、MC13の種別が判別されるまでは、図9と同様である。

【0081】ここでは、MC13の種別は、レベル1であるので、メディアI/F部6あるいはPD12は、その種別に応じたチェックイン/チェックアウト処理を実行する(ステップS5)。

【0082】チェックインの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介して、SMS2になされた場合、MC13の種別がレベル1であると判別されているので、その指示

は、拒否される。

【0083】チェックアウトの指示がLCM1のユーザインタフェース(I/F)部15を介して、あるいは、PD12を介して、SMS2になされた場合について、図13を参照して説明する。

【0084】SMS2は、宿帳のチェックアウト要求のあったコンテンツ(例えばコンテンツIDが「TID1」であるとする)の子の残数nを調べ(ステップS401)、n>0のとき、必要があれば、MC13との間で相互認証を行い(ステップS402)、相互に正当性が確認されたら、次に、MC13から、その識別情報MID(例えば、MID=m0とする)を転送してもらう(ステップS403)。

【0085】SMS2は、レベル2の場合と同様、乱数rの発生、暗号化鍵wの生成、コンテンツ鍵をwとKpを用いて暗号化、コンテンツCの暗号化を行い(ステップS404)、MC13の記憶領域(ここでは、公開領域のみ)に、例えば「TID1」という名前のフォルダを作成する(ステップS405)。そして、当該フォルダに暗号化されたコンテンツK(C)[C]と、暗号化されたコンテンツ復号鍵w[Kp[k(C)]]と乱数rとを書き込む(ステップS406～ステップS408)。

【0086】最後に、SMS2は、図7(b)に示すように、宿帳のチェックアウト要求のあったコンテンツID「TID1」のコンテンツの子の残数nから「1」減算し、チェックアウトリストL1に、当該MC13の識別情報「m0」を追加する(ステップS409)。

【0087】次に、レベル1のMC13に記憶された複製コンテンツの再生について、図14を参照して説明する。MC13をPD12にセットすると、PD12は、MC13から、その識別情報MID(例えば、MID=m0とする)を転送してもらう(ステップS501)。このとき、識別情報MID=m0を基に、MC13の種別を判別が、レベル1であることが判別できる。そこで、PD12は、MC13の記憶領域(公開領域のみ)からw[Kp[k(C)]]、乱数rを読み出し(ステップS502～ステップS503)、乱数rと、MC13の識別情報m0と、正当なるMC13とPD12との間で共有する鍵生成アルゴリズムWを用いて、暗号化鍵wを生成する。暗号化鍵wと、MC13とLCM1との間で共有する暗号鍵Kpと、MC13から読み出されたw[Kp[k(C)]]とからコンテンツ復号鍵K(C)を復号する(ステップS504)。

【0088】そして、PD12は、MC13の記憶領域(公開領域のみ)から暗号化されたコンテンツK(C)[C]を読み出し(ステップS505)、復号部12gでコンテンツCを復号し、デコーダ12hでデコードして、D/A変換部でデジタル信号からアナログ信号に変換し、音楽を再生する(ステップS506)。

【0089】(レベル0のMCを用いた複製コンテンツのチェックイン／チェックアウト、複製コンテンツの再生)次に、図4(a)に示したような構成のレベル0のMC13を用いたチェックイン／チェックアウトについて、図9、図15～図16を参照して説明する。

【0090】レベル0のMC13は、PD12を用いてしかチェックイン／チェックアウトおよび再生が行えない。また、識別情報MIDを持たないため、代わりにチェックイン／チェックアウトにおいて、PD12の識別情報PIDが用いられる。

【0091】MC13がPD12にセットされてから、MC13の種別が判別されるまでは、図9と同様である。

【0092】ここでは、MC13の種別は、レベル0であるので、PD12は、その種別に応じたチェックイン／チェックアウト処理を実行する(ステップS4)。

【0093】チェックアウトの指示がPD12を介して、SMS2になされた場合について、図15を参照して説明する。

【0094】SMS2は、宿帳のチェックアウト要求のあったコンテンツ(例えばコンテンツIDが「TID1」であるとする)の子の残数 $n$ を調べ(ステップS601)、 $n > 0$ のとき、PD12との間で相互認証を行い(ステップS602)、相互に正当性が確認されたら、次に、PD12から、その識別情報PIDを転送してもらう(ステップS603)。

【0095】SMS2は、レベル2の場合と同様、乱数 $r$ の発生、暗号化鍵 $w$ の生成、コンテンツ鍵を $w$ と $K_p$ を用いて暗号化、コンテンツ $C$ の暗号化を行う(ステップS604)。但し、ここでは、鍵生成アルゴリズム $W$ のとり2つの引数は、 $r$ とPIDである。

【0096】次に、MC13の記憶領域(ここでは、公開領域のみ)に、例えば「TID1」という名前のフォルダを作成する(ステップS605)。そして、当該フォルダに暗号化されたコンテンツ $K(C)[C]$ と、暗号化されたコンテンツ復号鍵 $w[K_p[k(C)]]$ を書き込む(ステップS606～ステップS607)。乱数 $r$ は、PD12の秘匿領域に書き込む(ステップS608)。ステップS608において、乱数 $r$ をPD12の秘匿領域に転送するまでの経路は、乱数 $r$ を暗号化する等して転送保護することが望ましい。

【0097】最後に、SMS2は、図7(b)に示すように、宿帳のチェックアウト要求のあったコンテンツID「TID1」のコンテンツの子の残数 $n$ から「1」減算し、チェックアウトリスト $L1$ に、PD12の識別情報「PID」を追加する(ステップS609)。

【0098】チェックインの指示がPD12を介して、SMS2になされた場合について、図16を参照して説明する。

【0099】SMS2は、PD12との間で相互認証を

行い(ステップS701)、相互に正当性が確認されたら、次に、PD12から、その識別情報PIDを転送してもらう(ステップS702)。

【0100】SMS2は、チェックイン要求のなされたコンテンツ(例えばコンテンツIDが「TID1」であるとする)の宿帳から、そのチェックアウトリストに当該PD12の識別情報「PID」が登録されているとき、乱数 $r1$ 、 $r2$ を発生させる(ステップS703)。そして、MC13の公開領域13aの当該コンテンツのフォルダ(ここでは、フォルダ「TID1」)に対応する領域に記憶されている情報を乱数 $r2$ で上書きすることで消去し(ステップS704)、また、SMS2は、PD12の秘匿領域にアクセスすべく、PD12との間で相互認証を行い、双方の正当性が確認されて秘匿領域へのゲートが開かれると、秘匿領域13c内のフォルダ「TID1」に対応する領域を乱数 $r1$ で上書きすることで消去する(ステップS705)。それが終了すると秘匿領域へのアクセスを可能にしていたゲートが閉じられる。また、ステップS705において、乱数 $r1$ を秘匿領域に転送するまでの経路は、乱数 $r1$ を暗号化する等して転送保護することが望ましい。

【0101】その後、SMS2では、上書き消去の確認をすべく、MC13から上書き後の値を転送してもらい、また、PD12の秘匿領域からも上記所定の秘匿手続を行って、当該領域の上書き後の値を読み出し(ステップS706)、それが乱数 $r1$ 、 $r2$ と一致するかどうかチェックする(ステップS707)。上書き消去の確認がなされたら、MC13からフォルダ「TID1」を消去する(ステップS708)。

【0102】最後に、図7(c)に示すように、宿帳のチェックイン要求のあったコンテンツID「TID1」のコンテンツの子の残数 $n$ に「1」加算し、チェックアウトリスト $L1$ から、PD12の識別情報「PID」を削除する(ステップS709)。

【0103】次に、レベル0のMC13に記憶された複製コンテンツの再生について、図17を参照して説明する。MC13をPD12にセットすると、PD12は、MC13から、その識別情報MIDの転送を要求するが、MC13は、識別情報をもっていないので、PD12は、当該MC13は、レベル0であると判別できる。そこで、PD12は、MC13の記憶領域(公開領域のみ)から $w[K_p[k(C)]]$ を読み出し(ステップS801)、PD12自身の識別情報「PID」と、その秘匿領域に格納されている乱数 $r$ と鍵生成アルゴリズム $W$ とを用いて、暗号化鍵 $w$ を生成する。そして、暗号化鍵 $w$ と、暗号鍵 $K_p$ と、MC13から読み出された $w[K_p[k(C)]]$ とからコンテンツ復号鍵 $K(C)$ を復号する(ステップS802)。

【0104】PD12は、MC13の記憶領域(公開領域のみ)から暗号化されたコンテンツ $K(C)[C]$ を

読み出し（ステップS803）、復号部12gでコンテンツCを復号し、デコーダ12hでデコードして、D/A変換部でデジタル信号からアナログ信号に変換し、音楽を再生する（ステップS804）。

【0105】（ネットワークを介するMCへの複製コンテンツ記録を規制するための手段）本発明の2つ目の問題点を解決するために、すなわち、ネットワークを経由したコンテンツのMC13への記録を規制するために、本発明では、図1に示すようにタイムアウト判定部4を設けている。

【0106】タイムアウト判定部4では、MC13への読み書き（いずれか一方、又は両方）手順において、一定の制限時間を設定し、処理が制限時間内に終わらなければ処理を中断する。ネットワークを通じた通信は通常、直接接続された機器との通信に比較して遙かに長い時間を要する為、タイムアウト機能によって、ネットワークを通じた違法コピーに対抗する事ができる。又、帯域制限を用いる事もできる。機器との通信帯域を一定以上と仮定すれば、或るサイズのデータを機器に転送する際に要する時間の上限が計算できる。実際の転送時間が、それを上回った場合、処理を中断する。

【0107】図22に示すタイムアウト判定部4の構成と図23に示すフローチャートを参照して、もう少し具体的に述べる。予めタイムアウト時間 $t$ を設定することにし、例えば、LCM1とPD12との間の通信帯域幅を $b$ とする。例えば、PD12にセットされているMC13との間でチェックアウトを行う場合を例にとり、タイムアウト判定部4の処理動作について説明する。

【0108】まず、PD12にセットされているMC13との間のチェックアウトのための手順にあるある1つの読み書き処理動作の開始とともに、SMS2から判定開始信号入力部102を介して判定開始信号が入力し（ステップS20）、それとともに、SMS2からPD12との間でやりとりされるパケットデータのサイズ $s$ がデータサイズ入力部101から入力し（ステップS21）、制御部105は、時刻取得部106を介して時計107から現在時刻 $T$ を取得する（ステップS22）。これに伴って、帯域幅格納部108から帯域幅 $b$ を取得し（ステップS23）、終了予定時刻 $T'$ を算出して（ステップS24）。最終予定時刻格納部111に格納する（ステップS25）。

【0109】終了予定時刻 $T'$ は、帯域幅 $b$ とデータサイズ $s$ とから  $T' = T + s / b$  より求めることができる。

【0110】PD12にセットされているMC13との間の読み書き処理動作の終了とともに、SMS2から判定終了信号入力部103を介して判定終了信号が入力されると（ステップS26）、再び、現在時刻 $T$ を取得し（ステップS27）、先に算出された終了予定時刻 $T'$ と現在時刻 $T$ との差とタイムアウト時間 $t$ とを比較する

（ステップS28）。当該差がタイムアウト時間 $t$ を超えているときは、「NG」と判定し、その旨をSMS2へ通知する（ステップS30）。もし、PD12が図21に示したようにチェックアウトを行うPC#1にあるLCM1とネットワークにて接続された他のPC#2に接続されたものであるとすると、「NG」という判定結果が得られるので、PC#1のLCM1では、それ以降のチェックアウトのための処理を中断する。

【0111】あるいは、終了予定時刻 $T'$ が経過しても当該読み書き処理動作が終了していないとき、判定結果を「NG」としてもよい。

【0112】あるいは、タイムアウト判定部4は2つのモードで動作する。1つは、データサイズ入力部101にデータサイズ $s$ が入力されたときで、このとき、タイムアウト判定部は終了予定時刻 $T' = T + s / b$ を算出して、それを終了予定時刻格納部111に格納する。タイムアウト判定部4は、判定終了信号を受け取ると、現在時刻 $T$ と終了予定時刻格納部が格納する時刻 $T'$ とを比較する。前者が後者より小さい場合、タイムアウト判定部4は判定結果OKをSMS2に通知する。それ以外のときは、判定結果NGをSMS2に通知する。

【0113】他方のモードの動作は、判定開始信号入力部102に判定開始信号が入力された場合で、タイムアウト判定部4は、現在時刻 $T$ とタイムアウト時間 $t$ を終了予定時刻格納部111に格納する。タイムアウト判定の動作は上記一方のモードの場合と同様である。

【0114】（秘匿領域）本発明のLCM1では、チェックイン／チェックアウトのための宿帳を格納する為に、秘匿領域を利用する。LCM1をPCで構成する場合、この秘匿領域はハードディスク（HDD）上に作成される。

【0115】ここでは、HDD上の秘匿領域について説明する。

【0116】HDD上には通常パーティションが存在する。パーティションは、OSから1つのドライブとして認識される。各パーティション内に複数のセクターが存在し、データはセクター上に記録される。セクター内のデータ配置を論理フォーマットと呼ぶ。ファイルシステムは、通常ファイル配置テーブルを有する。ファイル配置テーブルには、各ファイル及びディレクトリのセクター上の位置が記録されている。OSは、ファイル配置テーブルを参照して、アクセス対象ファイルの位置を取得し、対象ファイルに到達する。セクターの物理的配置を物理フォーマットと呼ぶ。各パーティションは異なる物理フォーマットを有する事ができる。セクターの位置はヘッドの位置によって識別される。各セクターの開始位置は、磁気的なマークによって識別される。

【0117】OSがサポートするファイルシステムについて、OSはドライブを持っている。ドライブは当該ファイルシステムの物理フォーマット及び論理フォーマット

トを認識しており、パーティション内のセクターを辿ってファイル配置テーブルや各ファイルに到達し、その内容を読み書きする事ができる。

【0118】本発明の秘匿領域を構成するためのファイルシステムを図24に示す。通常のファイルシステムでは、セクターは等間隔に配置されるが、本ファイルシステムでは、そうになっていない。第1セクターの先頭には、セクター配置テーブルがある。セクター配置テーブルは次の形でセクター位置が記録されている。

【0119】

ヘッド位置#2、ヘッド位置#3、…、ヘッド位置#n順に、第2セクター、第3セクター、…、第nセクターの位置を示している。セクター配置テーブルは暗号化されている。この暗号化を解く鍵は、システムの固有IDに依存する。システム固有のIDとしては、例えばOSのID、BIOSのID或いはCPUのIDなどが用いられる。

【0120】更に、第2セクターの先頭には、ファイル配置テーブルが存在する。これは次の形式である。

【0121】

(ファイル1、(セクター番号、セクター内位置))、  
(ファイル2、(セクター番号、セクター内位置))、  
…

セクター内位置は、セクター先頭からのバイト数である。ファイル配置テーブルも又暗号化されている。この暗号鍵も又、システム固有のIDに依存している。

【0122】本発明のファイルシステムに対するアクセスは、特別なドライバ(図1の秘匿領域ドライバ7)を用いて行う。秘匿領域ドライバ7の動作を図25に示す。当該ドライバ7は又、セクター配置を変更する機能を有している。セクター配置更新時の秘匿領域ドライバ7の動作を図26に示す。

【0123】(認証)以上の説明において、例えば、LCM1にMC13をセットした際に行われる相互認証や、秘匿領域にアクセスする際に行われる認証処理の一例を挙げる。これは、従来からあるもので、公開鍵暗号方式を用いた認証であるが、本発明はこれに限定するものではない。

【0124】図20において、2つの機器(例えば、LCM1とMC13)間でAからAにアクセスしようとしているBを認証する場合について説明する。

【0125】この場合、機器Aは、公開鍵kpを保持しており、機器Aにアクセス可能であるならば、機器Bは、公開鍵kpに対応する秘密鍵ksを保持している。機器Bは、機器Aで発生された乱数Rを受け取ると、それを秘密鍵ksで暗号化して(ks[R]と表す)、ks[R]を機器Aに返す。機器Aでは、公開鍵を用いて、ks[R]を復号し、復号結果が先に発生した乱数Rに等しければ、機器Bは正しい相手であると判定する。

【0126】その後、上記と同じことを機器Bから機器Aに対して行うことで、相互認証を行うことができる。この場合、機器Bは公開鍵を保持し、機器Aは秘密鍵を保持し、機器Aが機器Bにて発生した乱数を秘密鍵で暗号化してそれを機器Bで公開鍵を用いて復号し、先に発生した乱数に等しいかを確認する。

【0127】

【発明の効果】以上説明したように、本発明によれば、複製コンテンツの数を効率よく規制して、コンテンツの著作権保護を可能にする。

【図面の簡単な説明】

【図1】本発明の実施形態に係る記憶媒体(メディア)に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム(LCM)の構成例を示した図。

【図2】メモリ領域の構成例を示した図。

【図3】記録再生装置(PD)の内部構成例を示した図。

【図4】3種類の記憶媒体の特徴を説明するための図。

【図5】メディアインタフェース(I/F)部の内部構成例を示した図。

【図6】チェックイン後の記憶媒体の記録内容を説明するための図。

【図7】LCMの秘匿領域に格納されている宿帳の記憶例を示した図。

【図8】LCMの秘匿領域に格納されている宿帳の他の記憶例を示した図。

【図9】チェックイン/チェックアウト処理手順を説明するためのフローチャートで、メディアの種別を判別して、その種別に応じた処理を選択するまでの手順を示したものである。

【図10】記憶媒体の種別がレベル2の場合のチェックアウト手順を説明するための図。

【図11】記憶媒体の種別がレベル2の場合のチェックイン手順を説明するための図。

【図12】記憶媒体の種別がレベル2の場合の再生手順を説明するための図。

【図13】記憶媒体の種別がレベル1の場合のチェックアウト手順を説明するための図。

【図14】記憶媒体の種別がレベル1の場合の再生手順を説明するための図。

【図15】記憶媒体の種別がレベル0の場合のチェックアウト手順を説明するための図。

【図16】記憶媒体の種別がレベル0の場合のチェックイン手順を説明するための図。

【図17】記憶媒体の種別がレベル0の場合の再生手順を説明するための図。

【図18】LCMの秘匿領域に格納されている宿帳のさらに他の記憶例を示した図で、フラグを含む宿帳を示したものである。

【図19】フラグを用いたチェックイン処理の概略を説明するためのフローチャート。

【図20】公開鍵暗号化方式を用いた認証手順を説明するための図。

【図21】ネットワークを介して記憶媒体への複製コンテンツの記録を行う場合の機器構成例を示した図。

【図22】タイムアウト判定部の内部構成例を示した図。

【図23】タイムアウト判定処理の一例を説明するためのフローチャート。

【図24】秘匿領域を構成するためのファイルシステムを説明するための図。

【図25】秘匿領域ドライバの動作を説明するためのフローチャート。

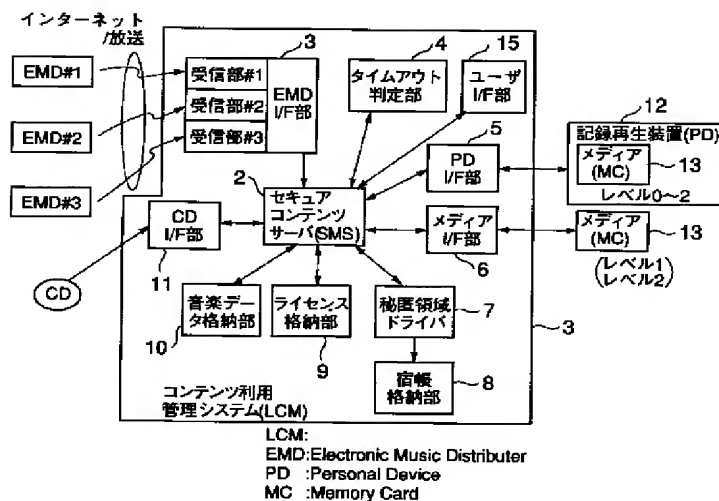
【図26】セクター配置更新時の秘匿領域ドライバの動

作を説明するためのフローチャート。

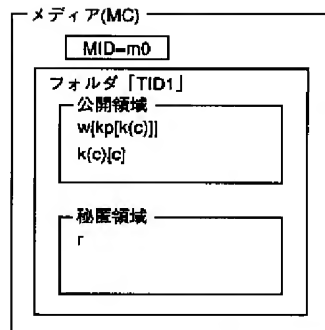
【符号の説明】

- 1…コンテンツ利用管理システム
- 2…セキュアコンテンツサーバ(SMS)
- 3…EMDインタフェース部
- 4…タイムアウト判定部
- 5…PDインタフェース(I/F)部
- 6…メディアインタフェース(I/F)部
- 7…秘匿領域ドライバ
- 8…宿帳格納部
- 9…ライセンス格納部
- 10…音楽データ格納部
- 11…CDインタフェース(I/F)部
- 12…記録再生装置(PD)
- 13…記憶媒体(MC)

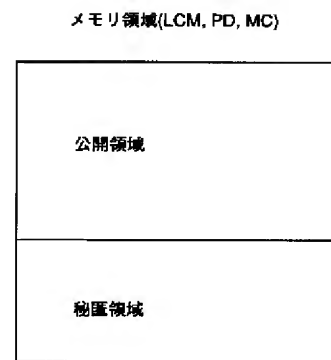
【図1】



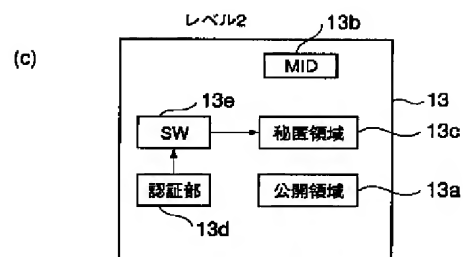
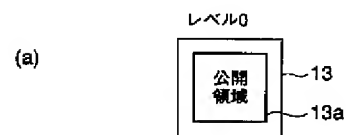
【図6】



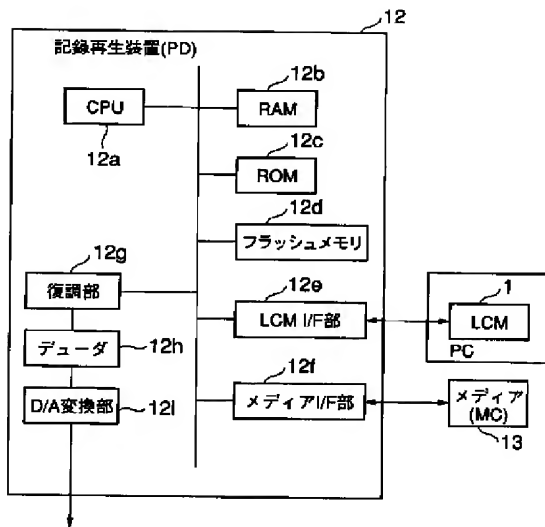
【図2】



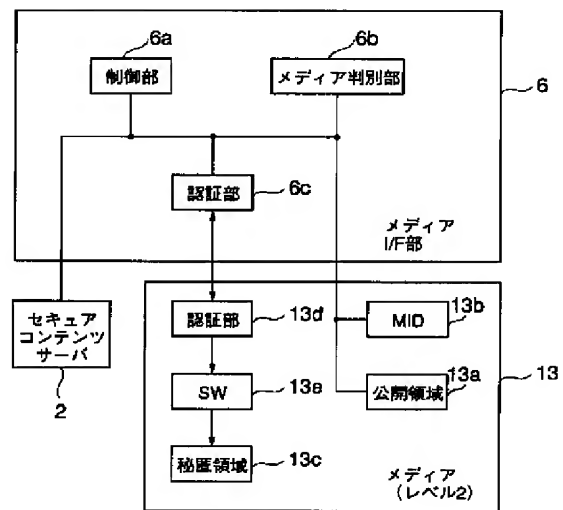
【図4】



【 3 】



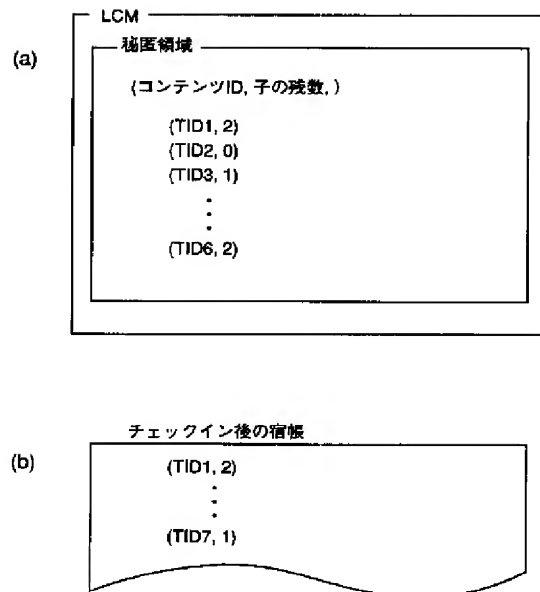
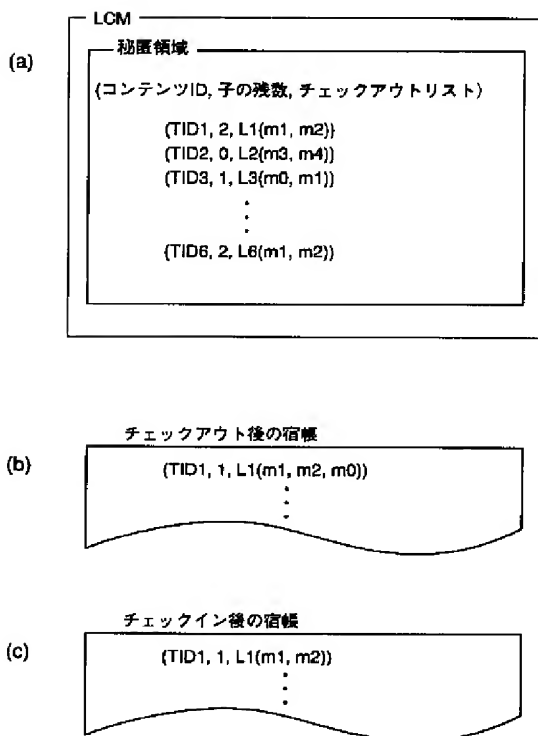
【 5 】



レベル1  
MIDのみ

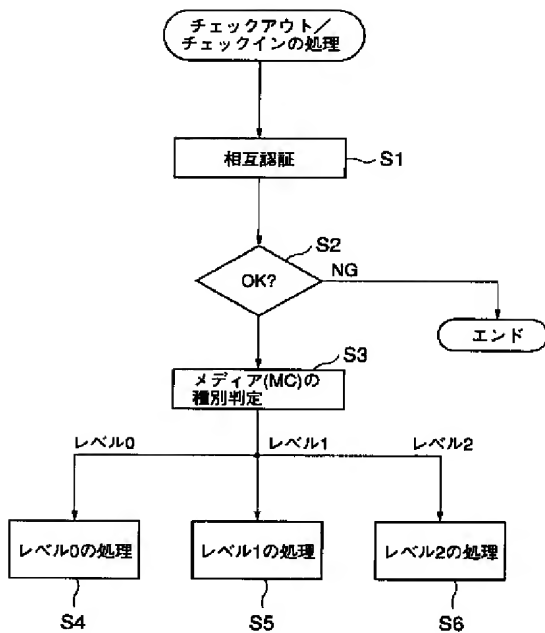
【 8 】

【 7 】

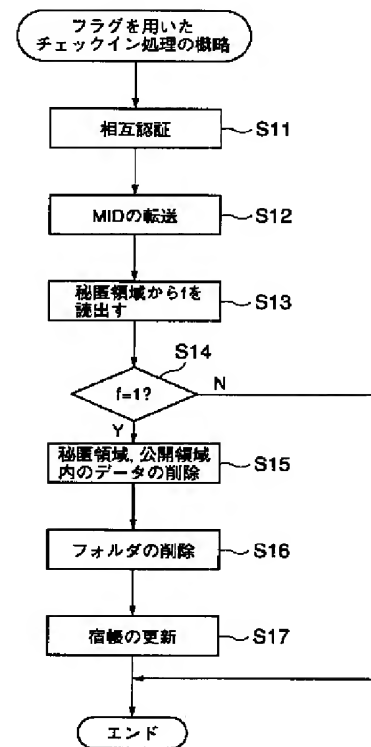




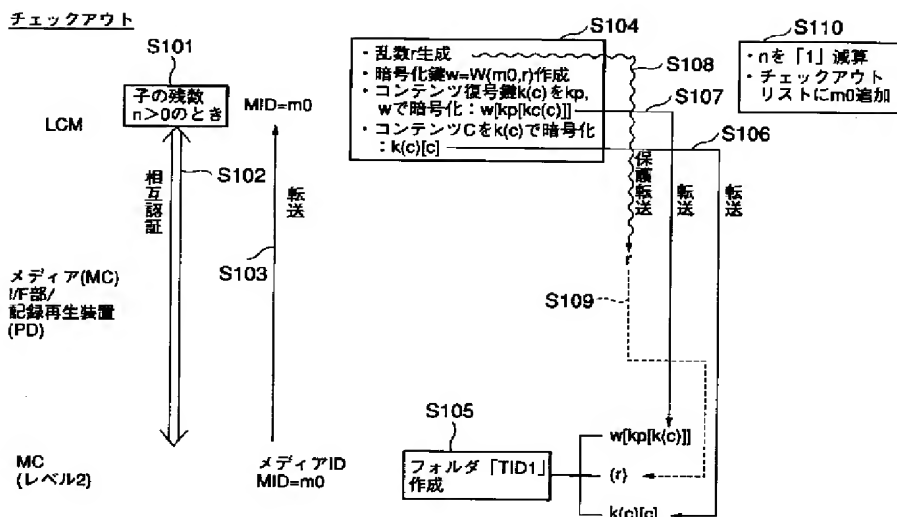
【図9】



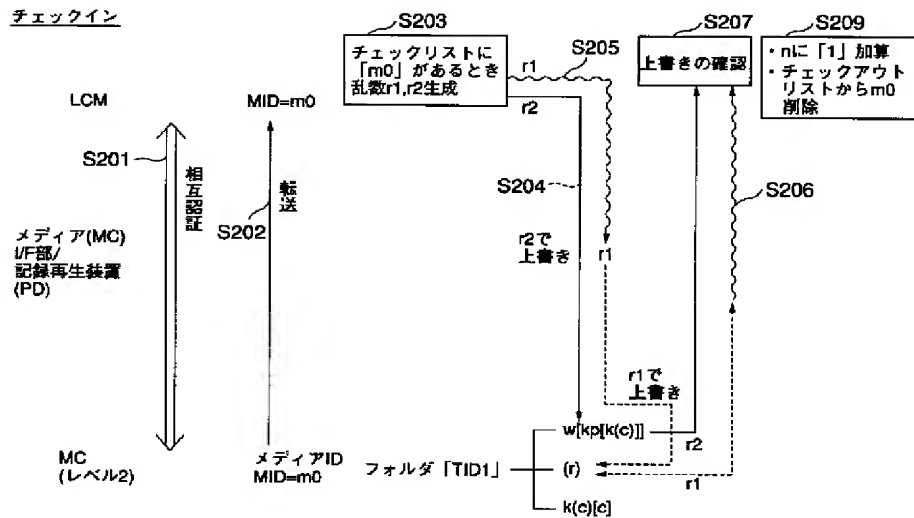
【図19】



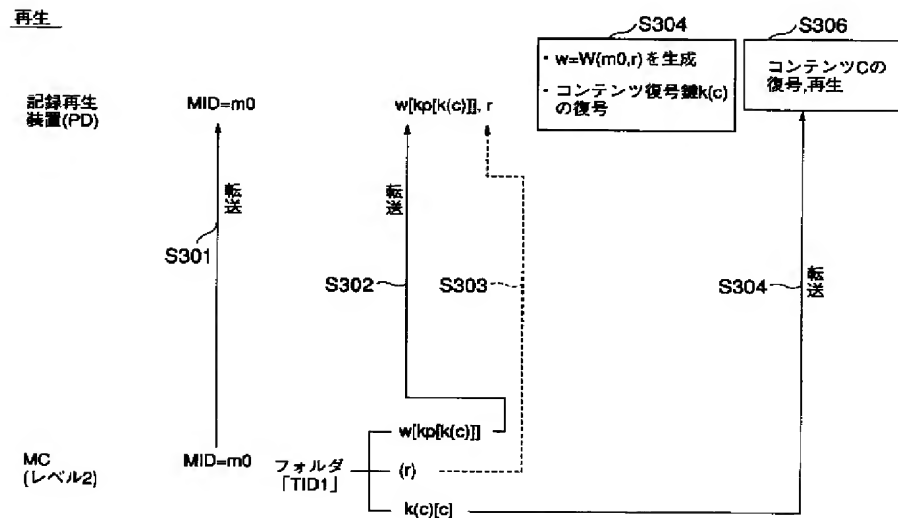
【図10】



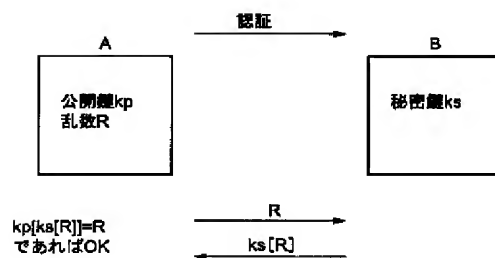
【图 1 1】



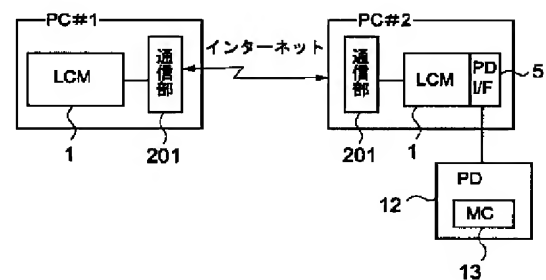
【例 12】



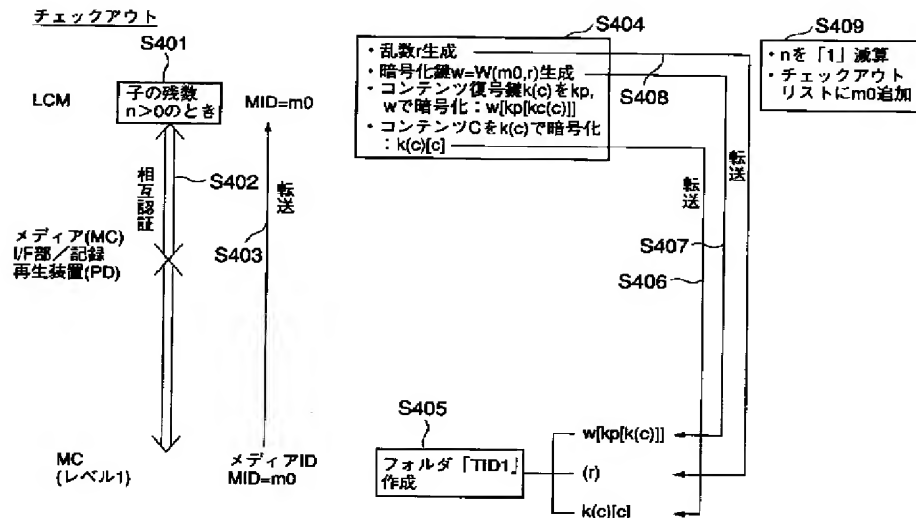
【図20】



【图 2 1】

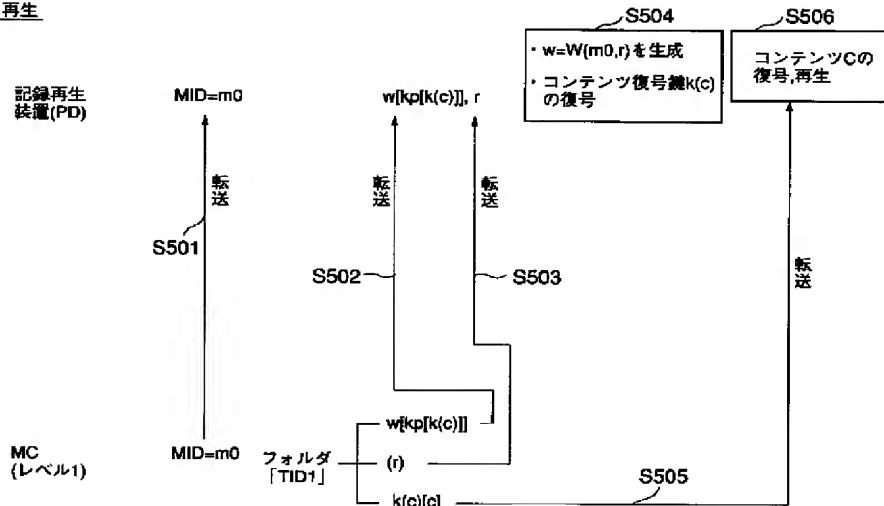


【図13】

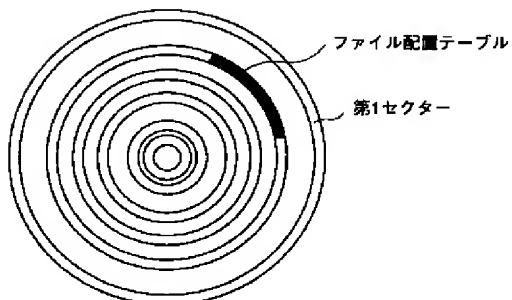


【図14】

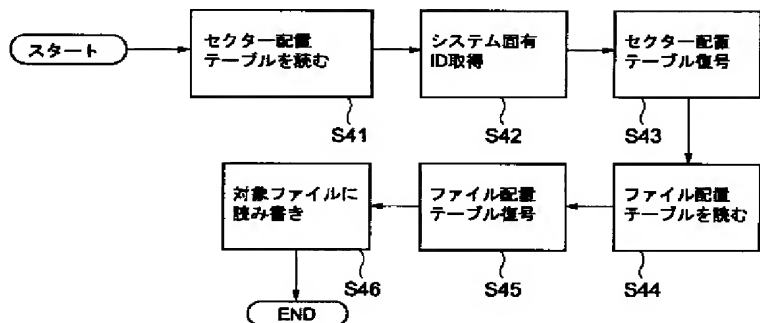
再生



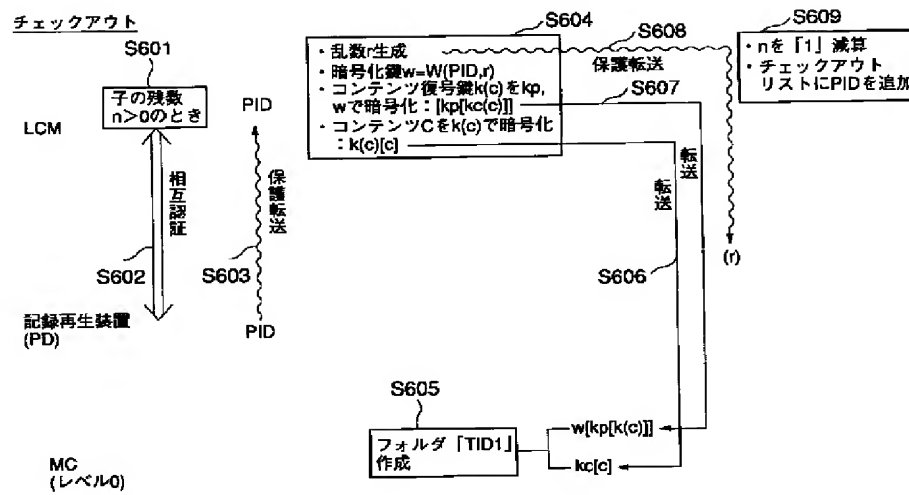
【図24】



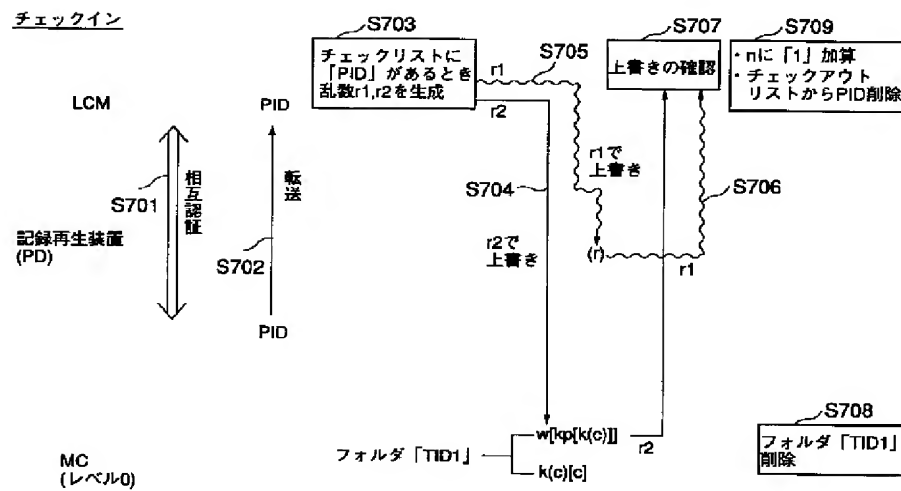
【図25】



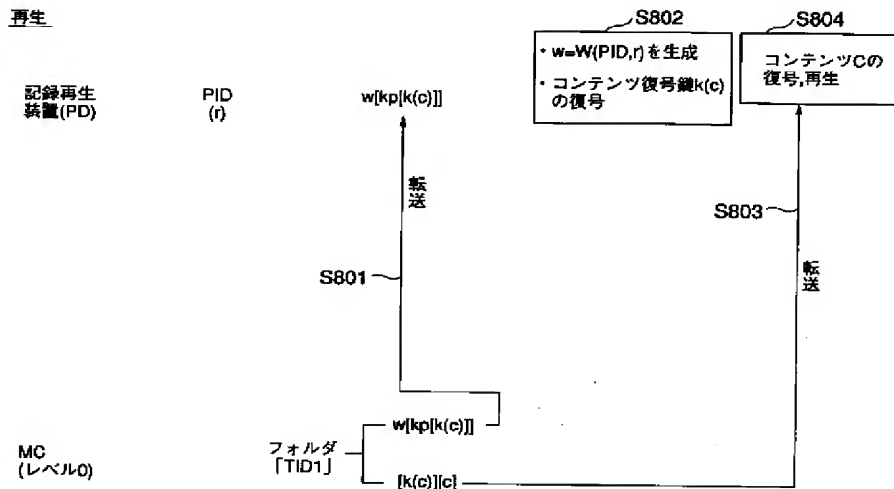
【図15】



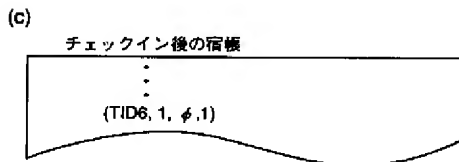
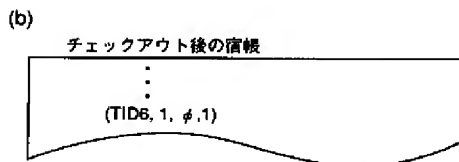
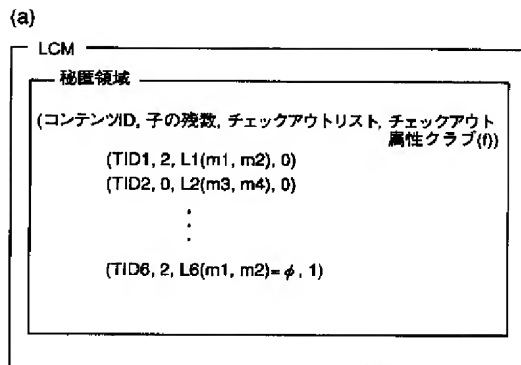
【図16】



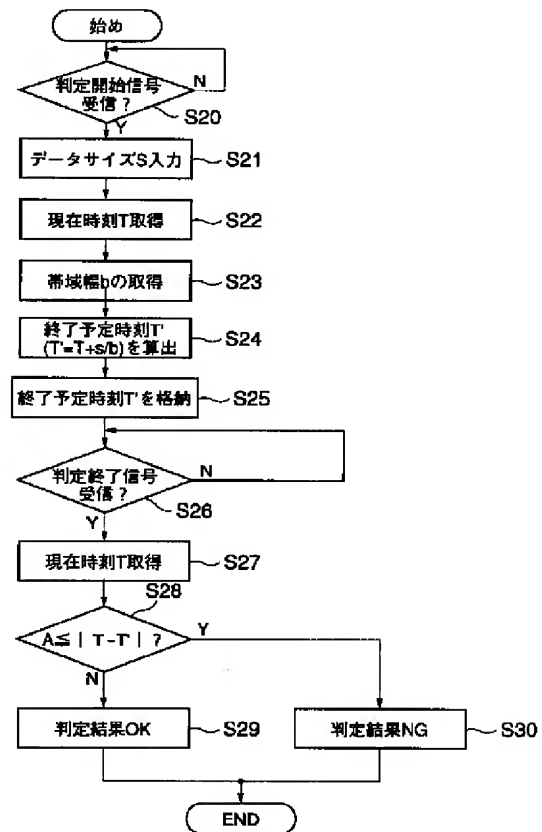
【図17】



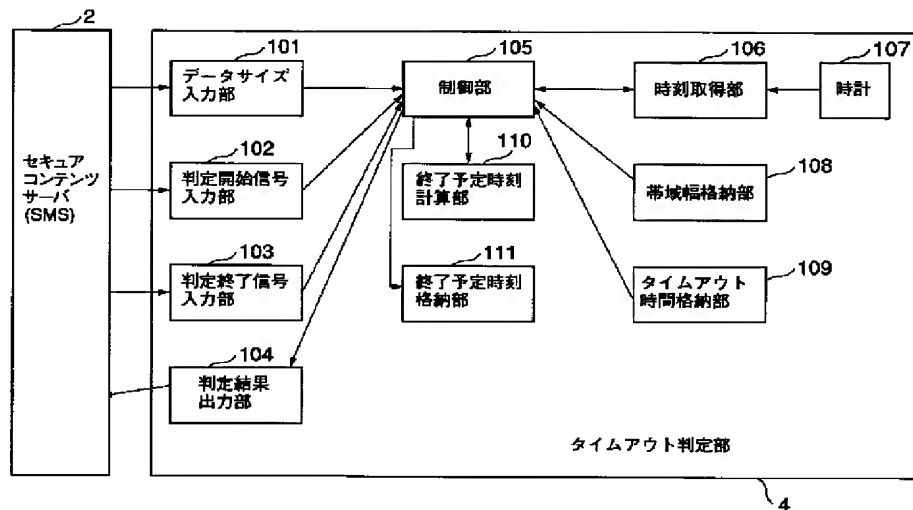
【図18】



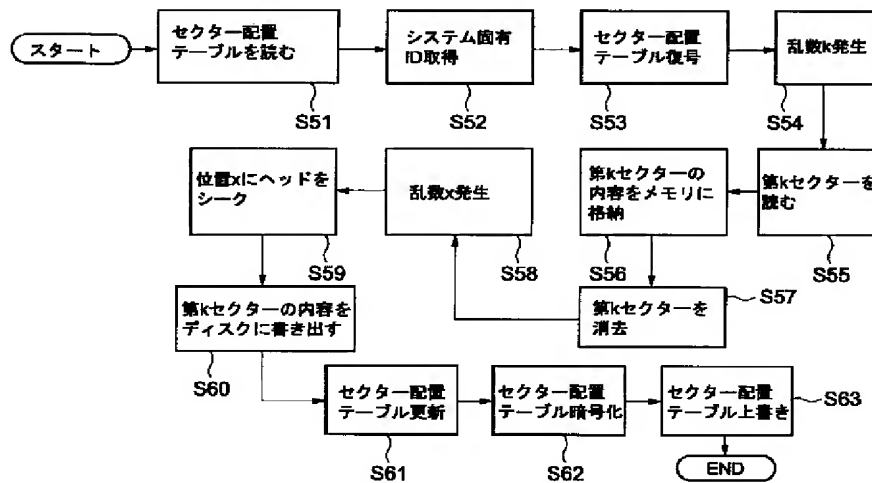
【図23】



【図22】



【図26】



フロントページの続き

(72)発明者 山田 尚志  
東京都港区芝浦一丁目1番1号 株式会社  
東芝本社事務所内

(72)発明者 石橋 泰博  
東京都青梅市末広町2丁目9番地 株式会  
社東芝青梅工場内

(72)発明者 加藤 拓  
東京都府中市東芝町1番地 株式会社東芝  
府中工場内

(72)発明者 東間 秀之  
東京都青梅市末広町2丁目9番地 株式会  
社東芝青梅工場内

Fターム(参考) 5B017 AA06 BA04 BA05 BA07 BA08  
BB10 CA07 CA08 CA09 CA13  
CA15 CA16  
5B075 KK54 KK68 ND16  
5C053 FA13 FA21 FA23 FA27 GB06  
GB11 HA29 JA01 JA21 KA04  
KA21 KA24 KA25 LA11 LA14